

Webinaire sensibilisation RGPD

Yohann FOURCHON, DPO ORU Bretagne
Emelyne PEYRAUD, DPO ORU Occitanie et ORU PACA



FEDORU
Fédération des Observatoires Régionaux des Urgences

Webinaire DPO
28 mai 2026

Protection des données (à caractère personnel)

Qu'est-ce qu'une donnée à caractère personnel :

- C'est toute information relative à une personne physique susceptible d'être identifiée directement ou indirectement ([w](https://video.cnil.fr/w/uRVbPWDW35bwHwWkXfXU47)



- <https://video.cnil.fr/w/uRVbPWDW35bwHwWkXfXU47>

I

(Actes législatifs)

RÈGLEMENTS

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 27 avril 2016

relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

(Texte présentant de l'intérêt pour l'EEE)

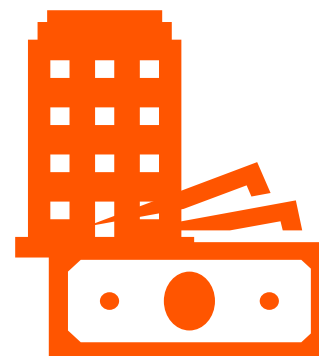
Quel périmètre pour le RGPD ?



Union
européenne



Public



Comme privé

- Autorité de contrôle de l'Etat français

- 4 missions :

- Informer / protéger les droits
- Accompagner la conformité et conseiller
- Anticiper et innover
- Contrôler et sanctionner

4 valeurs revendiquées

Indépendance

Conviction

Expertise

Collégialité

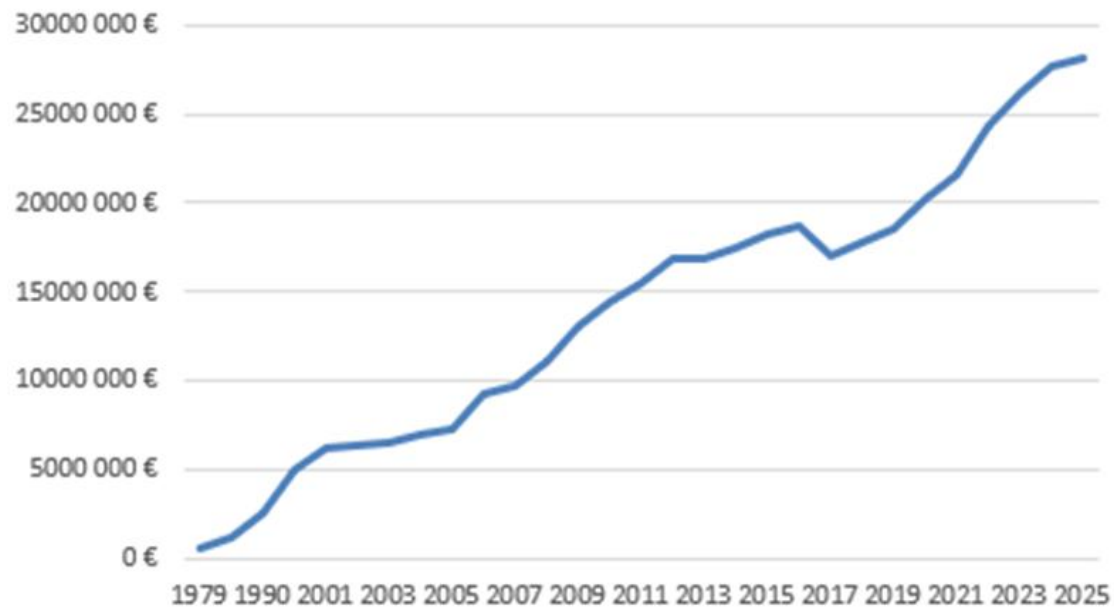


CNIL : Commission Nationale de l'Informatique et des Libertés

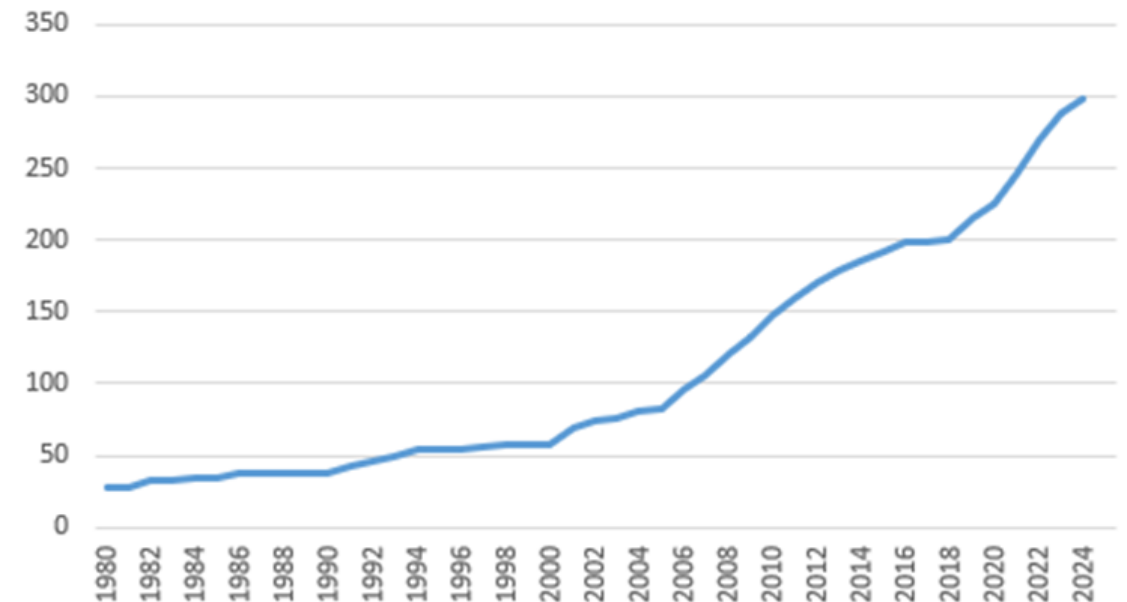


- Chiffres clés

CNIL : Budget total



CNIL : évolution des effectifs



Le DPO (ou DPD) – Délégué à la protection des données

Chef d'orchestre de la conformité RGPD

Qui doit déclarer un DPO ?



Notamment dès qu'il y a un traitement de données sensibles à grande échelle donc... tous les ORU !

Quelles missions ?



Accompagne et
veille à la
conformité
RGPD



S'assure de la
bonne tenue de
la documentation



Sensibilise et
conseille les
collaborateurs



Interlocuteur
privilegié de la
CNIL

Le Responsable de traitement

Responsable de la conformité RGPD

Qui est le responsable de traitement ?

Celui qui détermine les finalités et qui définit les moyens mis en œuvre

Quelles sont ses responsabilités ?

Il est garant de la conformité RGPD

Il contractualise avec ses sous-traitants (clauses contractuelles) en précisant ses instructions documentées

Il rend compte à l'autorité de contrôle (CNIL)

Les grands principes :

- Licéité, loyauté, transparence
- Finalités déterminées, explicites et légitimes
- Collectes adéquates, pertinentes et limitées
- Traitement sécurisé



Licéité : les 6 bases légales du traitement

© le consentement de la personne concerné ;



© le contrat : le traitement est nécessaire à l'exécution ou à la préparation d'un contrat avec la personne concernée ;



© l'obligation légale : imposé par des textes légaux ;



Licéité : les 6 bases légales du traitement

© la mission d'intérêt public : exécution d'une mission d'intérêt public ;



© l'intérêt légitime : intérêts légitimes de l'organisme qui traite les données ou d'un tiers, dans le strict respect des droits et intérêts des personnes concernées ;



hors autorité publique

© la sauvegarde des intérêts vitaux : le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, ou d'un tiers.



Les collectes des données doivent être :

- © Adéquates (*avec les besoins poursuivis par le traitement*)
- © Pertinentes (*nécessaire pour la bonne exécution du traitement*)
- © Limitées (*au strict nécessaire*)



La donnée de santé à caractère personnel :

- © Données sensibles (*recueil et traitement interdit par défaut*)
- © NIR (Numéro d'Inscription au Répertoire) = n° Sécurité Sociale
- © INS : Identité Nationale de Santé

Anonymisation vs pseudonymisation

Anonymisation	<u>Pseudonymisation</u>
Processus irréversible	Processus réversible
Impossibilité d'identifier directement ou indirectement une personne physique	Mesure de protection (<i>limitation du risque</i>) Identification possible par croisement de données
RGPD non applicable <i>si réévaluation régulière</i>	RGPD applicable
Avis du 10/04/2014 (G29)	Ligne directrice CEPD du 17/01/2025

Anonymisation vs pseudonymisation – Se poser les bonnes questions



Est-ce que je peux isoler un individu dans un jeu de données ?

Une base de données de CV où seuls les nom et prénoms d'une personne auront été remplacés par un numéro (qui ne correspond qu'à elle) permet d'individualiser cette personne



Est-ce que je peux relier deux ensembles de données distincts concernant un même individu ?

Une base de données cartographique renseignant les adresses de domiciles de particuliers ne peut être considérée comme anonyme si d'autres bases de données, existantes par ailleurs, contiennent ces mêmes adresses avec d'autres données permettant d'identifier les individus.



Est-ce que je peux déduire de façon quasi certaine de nouvelles informations sur un individu ?

Si un jeu de données contient des informations sur le montant des impôts de personnes ayant répondu à un questionnaire, que tous les hommes ayant entre 20 et 25 ans qui ont répondu sont non imposables. Si on sait que M. X, homme âgé de 24 ans, a répondu au questionnaire, on déduit que ce dernier est non imposable.

Anonymisation vs pseudonymisation



En pratique, la formation restreinte a relevé que la société CEGEDIM SANTÉ collectait de très nombreuses données sur les personnes concernées, telles que l'année de naissance, le sexe, la catégorie socio-professionnelle, les allergies, les antécédents médicaux, la taille, le poids, le diagnostic, les prescriptions médicales, les arrêts de travail et les résultats d'analyse. Ces données étaient reliées à un identifiant unique pour chaque patient d'un même médecin, permettant de relier entre elles les données transmises successivement par un même médecin concernant ce même patient et de reconstituer ainsi son parcours de soins. Au vu de ces éléments, la formation restreinte a considéré qu'**il est possible d'isoler un individu au sein de la base de données** de la société et que la société **dispose de nombreuses informations particulièrement riches** le concernant, ce qui induit un **risque de réidentification**.

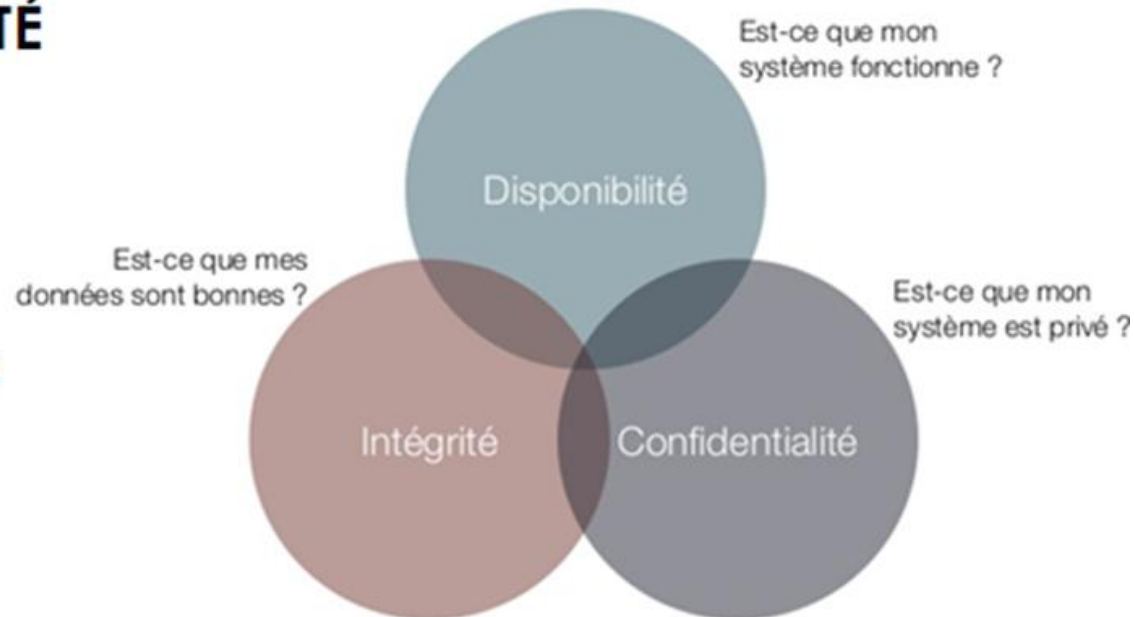
Sécurité du traitement de données

Les trois critères fondamentaux de la sécurité de l'information sont :

- ▶ **La CONFIDENTIALITÉ**
- ▶ **L'INTÉGRITÉ**
- ▶ **La DISPONIBILITÉ**

Sont aussi retenues :

- ▶ **L'IMPUTABILITÉ**
- ▶ **La TRAÇABILITÉ
(LA PREUVE)**



Les droits des personnes prévus par le RGPD



Droit d'accès



Droit à l'effacement
(ou droit à l'oubli)



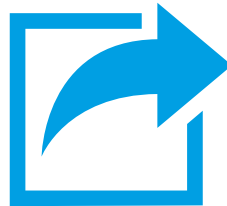
Droit à la
modification



Droit à
l'opposition



Retrait du
consentement



Portabilité



Limitation du
traitement

Documenter la conformité



Déclarer un
DPO



Registre de
traitement



Note
d'informations



Contrat



Analyse
d'impact ou
AIPD ou PIA

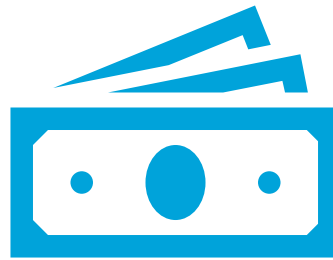
Quels risques ?



Quels risques ?



Publicité de la
sanction



Jusqu'à 10 millions €



5 ans
d'emprisonnement

Partie 2 – Traiter les données de santé

	RPU	RPIS (à partir du 1 ^{er} juillet 2027)
Base légale	<u>Arrêté du 24 juillet 2013 relatif au recueil et au traitement des données d'activité médicale produites par les établissements de santé publics ou privés ayant une activité de médecine d'urgence</u>	<u>Arrêté 9 avril 2026 relatif au recueil des données d'activité des structures mobiles d'urgence et de réanimation dans le cadre du résumé patient d'intervention SMUR</u>
Minimisation	Pseudonymisation de la base : • Suppression du nom de la commune de résidence • Remplacement du code INSEE par un code géographique • Remplacement de la DDN par l'âge à la date de l'intervention	
Qui informe ?	Etablissements siège de service d'urgence	« délivrée par les établissements de santé sièges de structures mobile d'urgence et de réanimation » et disponible sur les sites internet des établissements, de l'ATIH et des ARS
Quels droits sont applicables ?	Accès Rectification Limitation	
Où exercer ses droits ?	Auprès des établissements sièges de service d'urgence	Auprès des établissements sièges de SMUR

Partie 2 – Traiter les données à caractère personnel



Finalité



Base légale
ou fondement
juridique



Minimisation



Durée de
conservation



Droits des
personnes



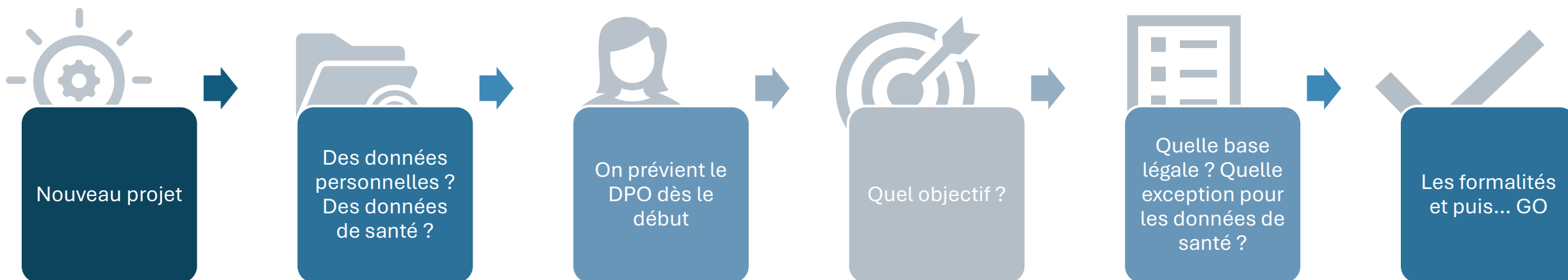
Sécurité



Respecter toutes les formalités

Et pour le reste ?

Et les autres données ? Que fait-on des RPU V3, hélismur, plus de données SMUR, voire des données des maisons médicales de garde ?



Trouver un consensus entre l'ensemble des ORU pour l'encadrement des données de santé en dehors de l'encadrement réglementaire !



Ne jamais oublier de contacter le DPO pour rester en conformité !

Merci pour votre attention !



FEDORU
Fédération des Observatoires Régionaux des Urgences